Wireless Two-Way Electronic Mail Desktop Protection Profile

FINAL DRAFT
Version 1.0

June 2002

Prepared By: Tresys Technology

Prepared For: Department of Defense

Disclaimer

This is a work in-progress document and subject to change. This draft document is not an official DoD document and its content is not binding until officially approved.

Foreword

This publication, *Wireless Two-Way Electronic Mail Desktop Protection Profile*, is issued by the National Security Agency (V34) program office as part of its program to support the next generation of wireless technologies. This protection profile is based on the “Common Criteria for Information Technology Security Evaluations, Version 2.1.”

Comments on this document should be directed to: Timothy Havighurst, NSA V34. The comments should include the title of the document, the page and paragraph number, detailed comment and recommendations.

Table of Contents

FOREWORD I

TABLE OF CONTENTS II

LIST OF TABLES AND FIGURES IV

1 INTRODUCTION 1

1.1 IDENTIFICATION 1
1.2 PROTECTION PROFILE OVERVIEW 1
1.3 CONVENTIONS 1
1.3.1 Operations on Components 1
1.3.2 Naming Conventions 3
1.4 GLOSSARY OF TERMS 3
1.5 DOCUMENT ORGANIZATION 4

2 TOE DESCRIPTION 5

3 TOE SECURITY ENVIRONMENT 7

3.1 SECURE USAGE ASSUMPTIONS 7
3.2 THREATS TO SECURITY 7
3.3 ORGANIZATIONAL SECURITY POLICIES 7

4 SECURITY OBJECTIVES 9

4.1 SECURITY OBJECTIVES FOR THE TOE 9
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 10

5 IT SECURITY REQUIREMENTS 12

5.1 SECURITY FUNCTIONAL REQUIREMENTS 12
5.1.1 STRENGTH OF FUNCTION CLAIMS 12
5.1.2 TOE Security Functional Requirements 12
5.1.3 Security Requirements for the IT Environment 20
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 20
5.2.1 Configuration items (ACM_CAP.2) 21
5.2.2 Delivery procedures (ADO_DEL.1) 22
5.2.3 Installation, generation, and start-up procedures (ADO_IGS.1) 22
5.2.4 Informal functional specification (ADV_FSP.1) 23
5.2.5 Descriptive high-level design (ADV_HLD.1) 23
5.2.6 Informal correspondence demonstration (ADV_RCR.1) 24
5.2.7 Administrator guidance (AGD_ADM.1) 25
5.2.8 User guidance (AGD_USR.1) 26
5.2.9 Analysis of coverage (ATE_COV.2) 27
5.2.10 Functional testing (ATE_FUN.1) 27
5.2.11 Independent testing - sample (ATE_IND.2) 28
5.2.12 Strength of TOE security function evaluation (AVA_SOF.1) 29
5.2.13 Independent vulnerability analysis (AVA_VLA.1) 29

6 RATIONALE 31

6.1 SECURITY OBJECTIVES RATIONALE 31
6.2 SECURITY REQUIREMENTS RATIONALE 35
6.2.1 TOE Assurance Requirements 35
6.2.2 Strength of Function Rationale 35

6.2.3 Dependency Satisfaction 35
6.2.4 Traceability 35
6.2.5 Suitability 36
6.2.6 Explicit Requirements Rationale 39

7 ACRONYMS 40

8 REFERENCES 41

9 ACRONYMS 43

10 REFERENCES 44

List of Tables and Figures

Table 1 Functional Requirements Operation Conventions 2
Table 2 TOE Assumptions 7
Table 3 Threats 7
Table 4 Organizational Security Policies 8
Table 5 Security Objectives for the TOE 9
Table 6 Security Objectives for the Environment 10
Table 7 TOE Security Functional Requirements 13
Table 8 Security Requirements for the IT Environment 20
Table 9 TOE Assurance Requirements 21

1 Introduction

This section contains overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The PP identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The conventions section provides an explanation of how this document is organized and the glossary of terms section gives a basic definition of terms, which are specific to this PP.

1.1 Identification

Title:	Wireless Two-Way Electronic Mail Desktop Protection Profile, Draft Version 1.0, June 2002
Authors:	Kimberly Caplan, Jandria Alexander (Tresys Technology)
Vetting Status:	Draft
CC Version	2.1
Evaluation Level:	Evaluation Assurance Level (EAL) 2
General Status:	Draft
Registration:	TBD
Keywords:	Wireless, Handheld, S/MIME, PKI, mail, mail server, desktop

1.2 Protection Profile Overview

This PP is one of three profiles that are used to specify information security requirements for the wireless two-way email solution. This PP specifies security requirements for the Desktop component and includes the evaluation assurance level (EAL) 2 assurance requirements, as defined by the Common Criteria. The Desktop provides a link between the Handheld and the user's email server(s). The Desktop participates in the synchronization of an email user's handheld mailbox with the desktop mailbox and maintains message status and settings on the desktop.

1.3 Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the CC. Font style and clarifying information conventions were developed to aid the reader.

1.3.1 Operations on Components

The CC permits four component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. Refinement and iteration operations can be performed on assurance requirements. These operations are defined in CC, Part 2, paragraph 2.1.4 as

- assignment: allows the specification of an identified parameter;
- iteration: allows a component to be used more than once with varying operations;
- refinement: allows the addition of details; and
- selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicized, and underlined text.

Uncompleted *assignments and selections* are indicated by brackets ("[ ]") to set off all assignments or selections that require future action by the developer to prepare a Security Target (ST). The text " ST Assignment:" or " ST Selection:" is indicated within the brackets.

Refinements are identified by bold text.

Iterations are identified with a number inside parenthesis ("(#)"). These follow the short component and functional element names.

Explicit Requirements are allowed to create requirements should the CC not offer suitable requirements to meet the PP needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating these requirements. The naming convention for explicit requirements is the same as that used in the CC. To ensure these requirements are explicitly identified, the ending "_EXP" is appended to the newly created short name. The newly created explicit requirements are integrated with the CC requirements and shown in bold text. The rationale for creating a requirement is provided in Section 6.2.6 Explicit Requirements Rationale.

Table 1 Functional Requirements Operation Conventions illustrates the operations as they are used in this PP.

Table 1 Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	The purpose of bolded text is used to alert the reader that additional text has been added to the CC requirement. Example: The TSF shall export **(in ASCII format)** the **labeled** user data with the user data's associated security attributes.	Assignment Refinement

Convention	Purpose	Operation
Italics	The purpose of italicized text is to inform the reader of an assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [*ST Assignment: list of additional SFP capabilities*].	Assignment Selection
Parentheses	The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times.	Iteration
Underline	The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to prevent modifications to the audit records.	Selection

Application notes provide support information that is considered relevant or useful for the construction, evaluation, or use of the Target of Evaluation (TOE). Application notes clarify the intent of a requirement, identify implementation choices, or define "pass-fail" criteria for a requirement. Application notes follow the relevant requirement component, are directive in nature, and may amplify the CC terminology stated in a specific requirement.

1.3.2 Naming Conventions

Assumptions: TOE security environment assumptions are given names beginning with "A." e.g., A.COMPONENTS.

Threats: TOE security environment threats are given names beginning with "T." e.g., T.IMPORT.

Policies: TOE security environment policies are given names beginning with "P." e.g., P.COMPLY.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE." respectively e.g., O.DATA_PRO and OE.EMAIL.

1.4 Glossary of Terms

This profile uses the terms described in this section to aid in the application of the requirements:

Authorized user	A user who has been uniquely identified and authenticated. These users are considered to be

	legitimate users of the TOE.

1.5 Document Organization

Section 1 provides the introductory material for the PP.

Section 2 describes the Desktop (i.e. the TOE for this PP) and its general purpose.

Section 3 describes the expected environment for the Desktop. This section defines:

- Secure use assumptions that describe the presumptive conditions for secure use in the selected environment,
- Threats that are to be addressed by either the technical countermeasures implemented in the Desktop hardware or software or through the environmental controls, and
- Organizational policies that levy further requirements for secure operations.

Section 4 defines the security objectives for both the Desktop and its environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively, that must be satisfied by the Desktop technology and development teams, respectively.

Section 6 provides a rationale to demonstrate explicitly that the information technology security objectives satisfy the policies and threats. Arguments are provided for the security objectives being necessary to support policies and counter threats. The section then explains how the set of requirements are sufficient to meet each objective, and that each security objective is addressed by one or more component requirements. Therefore, the two aforementioned subsections provide arguments that the security objectives and security requirements are both necessary and sufficient, respectively and collectively, to meet the needs dictated by the policies and threats. Next, Section 6 provides arguments that address strength of function issues, choice of assurance requirements, and the use of explicitly stated requirements.

An acronym list is provided to define frequently used acronyms.

The reference section identifies background material used to prepare this PP.

2 TOE Description

The wireless two-way email solution provides a security enhanced electronic mail messaging solution for the remote monitoring, creation and distribution of mail messages. The two-way wireless e-mail solution includes several related components. They are the Handheld device, the Mail Server Interface, and the Desktop with docking cradle. Figure 1, Wireless Two-way Email Architecture Components, illustrates the relationships between the components. The Handheld device is a mobile device that allows users to receive, review, and send email messages remotely. The Mail Server Interface is responsible for administering policy for the users and devices and properly distributing email to and from the handheld. The Desktop and cradle provide the user with the functionality to synchronize the desktop mailbox with the handheld and to download approved software and policies. Features of the wireless two-way email solution include:

- A single email address such that a message sent from the handheld and a message sent from the desktop is not distinguishable.
- A protected end-to-end transmission link between the handheld and the protected enclave where the server and desktop are located.
- Use of S/MIME to provide secure mail messaging for sensitive but unclassified email.

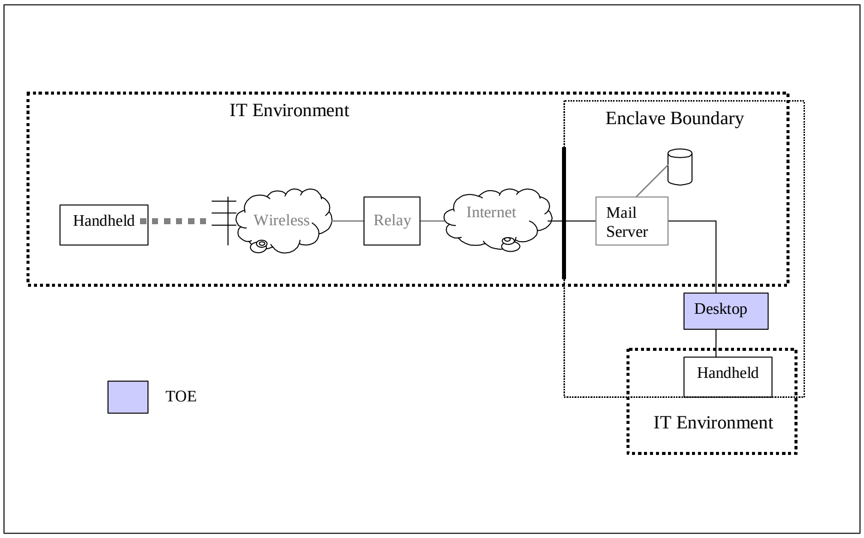

Figure 1 Wireless Two-way Email Architecture Components

Each component is specified in a separate PP and thus is a separate Target of Evaluation (TOE). Specifically, the TOE for this PP is the Desktop. The Handheld and Mail Server, as well as the communications network, are not part of the TOE and considered part of the information technology (IT) environment.

Figure 2 Wireless Two-way Email Architecture Components

The desktop provides the handheld user with the functionality to synchronize messages, contacts, appointments, memos, and tasks between the handheld and PC and generate an encryption key. The desktop software also allows the user to backup information from the handheld to the PC, edit the Address Book and AutoText files, restore data back to the handheld, configure email redirection settings, and load new applications onto the handheld.

The desktop operates within a protected enclave and provides a user interface for the email user to generate an encryption key for the communications between the desktop and the handheld, manage the user mailbox preferences and synchronize the desktop mailbox with the handheld mailbox. The desktop shall provide the following security services in its evaluated TOE configuration:

Identification and Authentication – the desktop user must be logged into the desktop prior to invoking desktop manager functionality.

Auditing – the desktop must audit user Identification and Authentication actions.

Self-Protection – The desktop provides domain separation and non-bypassability protection.

Data Protection – The TOE is responsible for generating an encryption key that is to be used to encrypt all mail traffic to the Handheld.

Security Management –The TOE must manage user accounts.

3 TOE Security Environment

The laws, organizational security policies, customs, expertise and knowledge that are relevant to the TOE define the security environment. The purpose of this section is to describe the nature and scope of security in which the TOE is intended to be used. The security environment is captured by security specific statements made about the TOE in terms of assumptions, threats, and applicable organizational security policies.

Subsequent sections of the PP and future STs show how the TOE, in combination with its operating environment, will address the security environment.

3.1 Secure Usage Assumptions

This section discusses the scope of intended usage of the TOE as well as assumptions about the operating environment including physical, personnel, and connectivity issues.

Table 2 TOE Assumptions

Name	Assumption
A.COMPONENTS	The Mail Server and Desktop operate within a protected enclave that provides protection against tampering and unauthorized physical access.
A.ENVIRON	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.IT_ENVIRON	The IT environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE.
A.TRAIN	Users are trained on the proper operations and procedures of the TOE.

3.2 Threats to Security

The TOE will provide protection against the threats listed in Table 3. These threats are actions that may have an adverse affect on the Desktop or its mission.

Table 3 Threats

Name	Threat
T.UNAUTH_ACCESS	An unauthorized user gains access to the TOE due to weak authentication controls.
T.UNAUTH_MOD	An unauthorized user modifies critical data.

3.3 Organizational Security Policies

Organizational security policies define a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4 identifies the organizational security policies applicable to the Desktop.

Table 4 Organizational Security Policies

Name	Policy
P.ACCOUNT	Users must be held accountable for security-relevant actions.
P.ACCESS	The system must limit access to information to those users who have the need to know that information.
P.COMPLY	The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization.
P.PROTECT	Encryption Keys transmitted must be protected.
P.DEDICATED	The TOE must be used for only purposes as specified by the organization.
P.GUIDANCE	Guidance must be provided for the secure installation and use of the system.
P.KNOWN	Users of the TOE must be identified and authenticated before access to TOE functions can be granted.
P.PASSWORD	Password based authentication mechanism must support a password space that allows alphanumeric, upper and lower case enforced symbols, a minimum password length of 8, and a feature to limit failed login attempts. Passwords shall not be echoed in a readable format.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 5 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified.

Table 5 Security Objectives for the TOE

Name	**TOE Security Objective**	**Corresponding Threat or Policy**
O.AUDIT	The TOE shall provide the capability to detect, create, store, and review records of security relevant events.	P.ACCOUNT
O.ACCESS	The TOE shall control access to the user's mailbox configuration status and data from the desktop based on the user's email identity and handheld identifier.	P.ACCESS
O.DATA_PRO	The TOE shall protect private key data transmitted from the TOE to other external components such as the Handheld and the mail server.	P.PROTECT T.UNAUTH.MOD
O.DOC	Guidance documentation provided to authorized users and administrators will detail the proper installation and use of the TOE to minimize the security risks within its intended environment.	P.GUIDANCE
O.EAL	The TOE must be structurally tested, shown to be resistant to obvious vulnerabilities, and be documented with sufficient design, test, and configuration documentation.	P.COMPLY
O.IDENTITY	The TOE shall uniquely identify and authenticate each user of the system. The TOE shall not allow any user actions to be performed before the TOE verifies the identity of the user.	P.KNOWN

Name	TOE Security Objective	Corresponding Threat or Policy
O.MANAGE	The TOE will provide adequate management features for its security functions and the wireless two-way email system.	P.DEDICATED
O.PASSWORD	The TOE will use an authentication mechanism that cannot be easily compromised in a low threat environment.	T.UNAUTH_ACCESS P.PASSWORD
O.SELF_PROTECT	The TOE must protect itself from unauthorized modification and access to its functions and data.	P.DEDICATED

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 6 identifies the security objectives for the environment.

Table 6 Security Objectives for the Environment

Name	Security Objective	Corresponding Assumption, Threat, or Policy
OE.COMPONENTS	Those responsible for the TOE must ensure the mail server and the desktop operate within a protective enclave.	A.COMPONENTS
OE.DEDICATED	Those responsible for the TOE must identify approved applications and software for the TOE to ensure that the TOE is used only for defined purposes.	P.DEDICATED P.COMPLY

Name	**Security Objective**	**Corresponding Assumption, Threat, or Policy**
OE.IT_ENVIRON	Those responsible for the TOE must ensure the TOE is used within an IT environment that does not contain vulnerabilities to undermine the secure operation of the TOE. Only approved network providers and public key infrastructures per organizational regulations shall be used.	A.IT_ENVIRON
OE.LOW_EXP	Those responsible for the TOE must ensure the TOE is used in an environment in which the threat of malicious attacks is low.	A.ENVIRON P.COMPLY
OE.TRAIN	Users are trained on the proper operations and procedures of the TOE.	A.TRAIN

5 IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC) and an EAL containing assurance components from Part 3 of the CC.

The functionality of a desktop *may* be implemented by more than one physical or logical component. The desktop could be implemented as an integrated mail desktop application executing on a commercial operating system or a dedicated hardware/software solution. This documents specifies functional and assurance security requirements for the desktop as a whole and does not attempt to separate requirements to influence implementations. Desktop implementations that use other components to satisfy the TOE requirements, should indicate that these requirements are allocated to the IT environment and do not need to be satisfied by the TOE. In this case, evidence must be provided that the IT environment separately satisfies requirements specified in Section 5.1.2 TOE Security Functional Requirements.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section provides information related to the TOE's Security Functional Requirements (SFRs). The first subsection addresses strength of function claims. The second subsection specifies the SFRs. The third subsection specifies the SARs.

5.1.1 STRENGTH OF FUNCTION CLAIMS

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. In the case of this protection profile, this minimum level shall be SOF-Basic.

Specific strength of function (SoF) metric is defined for FIA_UAU.1. Strength of function shall be demonstrated for the authentication mechanism such that for each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000.

5.1.2 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC summarized in Table 7.

Table 7 TOE Security Functional Requirements

Functional Component		Dependencies
FAU_GEN.1	Audit data generation	FPT_STM.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_STG.1	Protected audit trail storage	FAU_GEN.1
FDP_ACC.1	Subset access control	FDP_ACF.1
FDP_ACF.1	Security attribute based access control	FDP_ACC.1; FMT_MSA.3

FDP_UCT.1	Basic data exchange confidentiality	FTP_ITC or
		FTP_TRP;
		FDP_ACC.1 or
		FDP_IFC.1;

FDP_UIT.1	Data exchange integrity	FTP_ITC or
		FTP_TRP;
		FDP_ACC.1 or
		FDP_IFC.1;

FIA_UAU.1	Timing of authentication	FIA_UID.1
FIA_UID.1	Timing of identification	None
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1
FMT_MSA.3	Static attribute initialization	FMT_MSA.1; FMT_SMR.1
FMT_MTD.1(1)	Management of TSF data	FMT_SMR.1
FMT_MTD.1(2)	Management of TSF data	FMT_SMR.1
FMT_SMR.1	Security roles	FIA_UID.1
FPT_ITC.1	Inter-TSF confidentiality during transmission	None
FPT_RVM.1	Non-bypassability of the TSP	None
FPT_SEP.1	TSF domain separation	None
FPT_STM.1	Time stamps	None
FTP_ITC.1	Inter-TSF trusted channel	None

5.1.2.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and c)

- **User Logon attempts (successful and unsuccessful)**
- **Modification to Policy**
- **Administrative actions**
- **[ST assignment:** ***other specifically defined auditable events***].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [ST assignment: *other audit relevant informatio*n]

Dependencies:
FPT_STM.1 Reliable time stamps

5.1.2.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **the authorized administrator** with the capability to read **desktop audit information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies:
FAU_GEN.1 Audit data generation

5.1.2.3 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to <u>prevent</u> modifications to the audit records.

Dependencies:
FAU_GEN.1 Audit data generation

5.1.2.4 FDP_ACC.1 Subset access control

Hierarchical to: No other component

FDP_ACC.1.1 The TSF shall enforce the **email access control policy** on **individual user profiles, and associated email certificates and status among users and email profiles covered by the email access control policy**.

Dependencies:
FDP_ACF.1 Security attribute based access control

APPLICATION NOTE: This requirement establishes the policy to allow the desktop to read and write status information and certificates each desktop user.

5.1.2.5 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **email access control policy** to objects based on **user identity and profile attributes**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) desktop user will be granted full access to their mail box status, certificates and email after identification and authenticated to the desktop

b) [*ST Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*ST Assignment: rules, based on security attributes, that explicitly authorize access of subjects to object*s].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [*ST Assignment: rules, based on security attributes, that explicitly deny access of subjects to object*s].

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

APPLICATION NOTE: This requirement addresses the functionality for desktop to manage multiple user profiles and permit the user to access authorized mailbox data.

5.1.2.6 FDP_UCT.1Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the **email access control policy** to be able to <u>transmit, and receive</u> **private key** objects in a manner protected from unauthorized disclosure.

Dependencies:
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

APPLICATION NOTE: This requirement captures the need to protect private keys sent to other email components.

5.1.2.7 FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the **email access control policy** to be able to <u>transmit and receive</u> user **private key** data in a manner protected from <u>modification</u> errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user **private key** data, whether <u>modification</u> has occurred.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

APPLICATION NOTE: This requirement captures the need to protect private keys sent to and received from the other secure email components.

5.1.2.8 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow **no actions** on behalf of the user to be performed before the user is authenticated **to the Desktop**.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:
FIA_UID.1 Timing of identification

5.1.2.9 FIA_UID.1 Timing of Identification

Hierarchical to: No other components

FIA_UID.1.1 The TSF shall allow **no actions** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.2.10 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **email access control policy** to restrict the ability to <u>modify</u> the security attributes **user profile identity** to **the authorized administrator**.

Dependencies:
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

5.1.2.11 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **email access control policy** to provide <u>restrictive</u> default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **administrator** to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

APPLICATION NOTE: A user will not be able to access their desktop profile until after proper identification and authentication.

5.1.2.12 FMT_MTD.1(1) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(1) The TSF shall restrict the ability to add and delete the **user profiles** to **the authorized administrator.**

Dependencies:
FMT_SMR.1 Security roles

APPLICATION NOTE: This administrator must specify which users can maintain user profiles and email status on the desktop.

5.1.2.13 FMT_MTD.1(2) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(2) The TSF shall restrict the ability to define and modify **the desktop password policy for password length, character set, password expiration, and failed login attempt**s to the **authorized administrator.**

Dependencies:
FMT_SMR.1 Security roles

5.1.2.14 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the role **authorized administrator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

APPLICATION NOTE:

5.1.2.15 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

APPLICATION NOTE: This includes encryption keys generated on the Desktop and transmitted to the mail server and the handheld.

5.1.2.16 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

APPLICATION NOTE: The TOE must provide a security architecture such that all the functionality described by the TOE requirements in this PP cannot be bypassed. This means that the TOE should not have any external interfaces that can bypass the functionality described.

5.1.2.17 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.2.18 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

APPLICATION NOTE: This requirement applies to the timestamp placed on the stored audit records.

5.1.2.19 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF and the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transfer of policy, mail status and private keys.**

Dependencies: No dependencies

APPLICATION NOTE: The Desktop interacts with the Handheld and Mail server to transmit and receive policy, mail status and private keys. This requirement supports the concept that connectivity to secure email components must be trusted and thus protected.

5.1.3 Security Requirements for the IT Environment

This section identifies the IT security requirements that are to be met by the IT environment of the TOE (i.e., Handheld, Mail Server). The requirements identified in Table 8 are not all inclusive of the security requirement that the IT environment must satisfy but rather are those requirements in which the TOE depends upon for its correct operation. It should be noted that where security requirements for the IT environment refer to the TSF, they refer to the security functions of the environment not security functions of the TOE. Desktop implementations that use other components to satisfy the TOE requirements, should indicate that these requirements are allocated to the IT environment and do not need to be satisfied by the TOE. In this case, evidence must be provided that the IT environment separately satisfies requirements specified in Section 5.1.2 TOE Security Functional Requirements.

Table 8 Security Requirements for the IT Environment

Functional Component		Dependencies
FTP_ITC.1 (Handheld) (Mail Server)	Inter-TSF trusted channel	None
FPT_ITC.1 (Handheld, Mail Server)	Inter-TSF confidentiality during transmission	None

5.2 TOE Security Assurance Requirements

The TOE security assurance requirements, summarized in Table 9, detail the evidence and evaluation activities required for the Desktop to be used in the security environment described in this protection profile. Section 6 provides a justification for the chosen security assurance requirements and the selected EAL 2 assurance level.

Table 9 TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Configuration Items (ACM_CAP.2)
Delivery and Operations	Delivery procedures (ADO_DEL.1) Installation, generation, and start-up procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1) Descriptive high-level design (ADV_HLD.1) Informal correspondence demonstration (ADV_RCR.1)
Guidance documents	Administrator guidance (AGD_ADM.1) User guidance (AGD_USR.1)
Tests	Evidence of coverage (ATE_COV.1) Functional testing (ATE_FUN.1) Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Strength of TOE security function evaluation (AVA_SOF.1) Developer vulnerability analysis (AVA_VLA.1)

5.2.1 Configuration items (ACM_CAP.2)

Dependencies: No dependencies

Developer action elements:

ACM_CAP.2.1D. The developer shall provide a reference for the TOE.

ACM_CAP.2.2D. The developer shall use a Configuration Management (CM) system.

ACM_CAP.2.3D. The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C. The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C. The TOE shall be labeled with its reference.

ACM_CAP.2.3C. The CM documentation shall include a configuration list.

ACM_CAP.2.4C. The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C. The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C. The CM system shall uniquely identify all configuration items.

Evaluator action items:

ACM_CAP.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery procedures (ADO_DEL.1)

Dependencies: No dependencies

Developer action elements:

ADO_DEL.1.1D. The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D. The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action items:

ADO_DEL.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3 Installation, generation, and start-up procedures (ADO_IGS.1)

Dependencies:
AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D. The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action items:

ADO_IGS.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E. The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.4 Informal functional specification (ADV_FSP.1)

Dependencies:
ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.1.1D. The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C. The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C. The functional specification shall be internally consistent.

ADV_FSP.1.3C. The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C. The functional specification shall completely represent the TSF.

Evaluator action items:

ADV_FSP.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.5 Descriptive high-level design (ADV_HLD.1)

Dependencies:
ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.1.1D. The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C. The presentation of the high-level design shall be informal.

ADV_HLD.1.2C. The high-level design shall be internally consistent.

ADV_HLD.1.3C. The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C. The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C. The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C. The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C. The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action items:

ADV_HLD.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E. The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.6 Informal correspondence demonstration (ADV_RCR.1)

Dependencies: No dependencies

Developer action elements:

ADV_RCR.1.1D. The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C. For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action items:

ADV_RCR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: For this PP, this applies to ensure that the TOE summary specification contained in the Security Target and functional specification, functional specification and high-level design are consistent with each other.

5.2.7 Administrator guidance (AGD_ADM.1)

Dependencies:
ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D. The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C. The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C. The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C. The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C. The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C. The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C. The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_ADM.1.8C. The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

Evaluator action items:

AGD_ADM.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.8 User guidance (AGD_USR.1)

Dependencies:
ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D. The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C. The user guidance shall describe the functions and interfaces avail-able to the non-administrative users of the TOE.

AGD_USR.1.2C. The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C. The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C. The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C. The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C. The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

Evaluator action items:

AGD_USR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.9 Analysis of coverage (ATE_COV.2)

Dependencies:
ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D. The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C. The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action items:

ATE_COV.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.10 Functional testing (ATE_FUN.1)

Dependencies: No dependencies

Developer action elements:

ATE_FUN.1.1D. The developer shall test the TSF and document the results.

ATE_FUN.1.2D. The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C. The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C. The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C. The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C. The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C. The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action items:

ATE_FUN.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.11 Independent testing - sample (ATE_IND.2)

Dependencies:
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D. The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C. The TOE shall be suitable for testing.

ATE_IND.2.2C. The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action items:

ATE_IND.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E. The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E. The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Application Note: The choice of the subset tested and the sample tests executed is entirely at the discretion of the evaluator.

5.2.12 Strength of TOE security function evaluation (AVA_SOF.1)

Dependencies:
ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D. The developer shall perform a strength of TOE security function analysis for each mechanism identified in the Security Target (ST) as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C. For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C. For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action items:

AVA_SOF.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E. The evaluator shall confirm that the strength claims are correct.

5.2.13 Independent vulnerability analysis (AVA_VLA.1)

Dependencies:
ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.1.1D. The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D. The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C. The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action items:

AVA_VLA.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E. The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 Rationale

This section provides the rationale for the selection, creation, and use of security objectives and requirements.

6.1 Security Objectives Rationale

The security objectives rationale demonstrates that the stated security objectives (in Section 4) are traceable to all of the aspects identified in the TOE security environment (described in Section 3) and are suitable to cover them.

Table 5 in Section 4 shows that all security objectives for the TOE are traced back to aspects of the identified threats (in Section 3.2) and/or aspects of the organizational security policies to be met by the TOE (in Section 3.3). Table 6 in Section 4.0 shows that all security objectives for the environment are traced back to aspects of the organizational security policies and/or assumptions to be met by the TOE's environment. Table 10 presents the justification that the security objectives are suitable to counter the threats, and cover the OSP and assumptions described in Section 3.

Table 10 Security Objectives Justification

Threat/OSP/Assumption	**Security Objective(s)**	**Justification**
T.UNAUTH_ACCESS	O.IDENTITY O.PASSWORD	An unauthorized user gains access to the TOE due to weak authentication controls. O.IDENTITY and O.PASSWORD require the use of strong password mechanism and user identification before gaining access to the TOE.
T.UNAUTH_MOD	O.DATA_PRO	*An unauthorized user obtains private key data.* O.DATA_PRO levies the use of private key protection.
P.ACCOUNT	O.AUDIT O.IDENTITY	*Users must be held accountable for security-relevant actions.* Enforcement of this policy requires that users be identified (O.IDENTITY), that user actions be monitored, and that the resulting records of their actions be available for review (O.AUDIT).
P.ACCESS	O.ACCESS	*The system must limit access to information to those users who have*

Threat/OSP/Assumption	**Security Objective(s)**	**Justification**
		the need to know that information. O.ACCESS requires the TOE to restrict access to user profile such that the user is only able to access their assigned mailbox and private keys.
P.COMPLY	O.EAL OE.DEDICATED OE.LOW_EXP	*The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization.* O.EAL levies requirements on the TOE development and evaluation to be consistent with its intended use as prescribed by this PP. OE.DEDICATED is concerned with making sure administrator controls are in place to only have the TOE execute approved applications and OE.LOW_EXP ensures that the organization using the TOE only use the TOE in the intended environment prescribed by this PP and not for higher risk environments for which it was not designed.
P.PROTECT	O.DATA_PRO	*Private keys need to be protected when transmitted.* O.DATA_PRO levies the use of private key protection.
P.DEDICATED	O.MANAGE O.SELF_PROTECT OE.DEDICATED	*The TOE must be used only for purposes as specified by the organization to support the wireless two-way email system.* O.MANAGE requires that the TOE provide management features to support its operation. O.SELF_PROTECT levies requirements to only allow the use of authorized code for the TOE. OE.DEDICATED is concerned with having the TOE only execute approved applications.

Threat/OSP/Assumption	**Security Objective(s)**	**Justification**
P.GUIDANCE	O.DOC	*Guidance must be provided for the secure installation and use of the system.* O.DOC provides the guidance documentation required for proper installation, generation, and use of the TOE.
P.KNOWN	O.IDENTITY	*Users of the TOE must be identified and authenticated before access to TOE functions can be granted.* O.IDENTITY requires user identification and authentication, by the TOE before allowing access. O.IDENTITY does restrict the ability to perform actions before authentication.
P.PASSWORD	O.PASSWORD	*Password based authentication mechanism on the Desktop must support a password space that allows alphanumeric, upper and lower case enforced symbols, a minimum password length of 8, and a feature to limit failed login attempts.* O.PASS_POLICY levies requirements for the Desktop to enforce a password policy.
A.COMPONENTS	OE.COMPONENTS	*The Mail Server and Desktop operate within a protected enclave that provides protection against tampering and unauthorized physical access. The Handheld interacts properly with the Desktop.* OE.COMPONENTS levies requirements on those responsible for the TOE to ensure the Mail Server and Handheld components of the two-way email solution are protected.
A.ENVIRON	OE.LOW_EXP	*The threat of malicious attacks aimed at discovering exploitable*

Threat/OSP/Assumption	**Security Objective(s)**	**Justification**
		vulnerabilities is considered low. OE.LOW_EXP ensures that the TOE is only used in the intended environment and not for higher risk environments for which it was not designed.
A.IT_ENVIRON	OE.IT_ENVIRON	*The IT environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE.* Through procedural means, OE.IT_ENVIRON objective requires the maintainers of the TOE to properly install, configure, and operate the IT environment. Those responsible for TOE would avoid using the TOE in an IT environment known to be unstable or vulnerable to hostile attacks.
A.TRAIN	OE.TRAIN	*Users are trained on the proper operations and procedures of the TOE.* OE.TRAIN ensures authorized users are trained on security features of the system and how to use those features to properly protect mail.

6.2 Security Requirements Rationale

The security requirements rationale demonstrates that the set of security requirements (in Section 5) is suitable to meet and traceable to the security objectives (specified in Section 4). The set of IT security requirements are internally consistent because they were all derived from Part 2 and Part 3 of the CC, operations were performed in accordance to the CC, and the security requirements were chosen and written to apply to the same concepts expressed in the security objectives. The IT security requirements together form a mutually supportive whole because they were derived from the TOE security objectives, include FPT_RVM.1, and FPT_SEP.1 to prevent bypassing and unauthorized modification of the TSF, and include security management requirements to properly manage the security functions.

6.2.1 TOE Assurance Requirements

This protection profile has been developed for a basic robustness environment. Given consideration to best commercial practices for COTS products and assurance requirements for the various assurance levels, it was determined that EAL 2 was achievable and the most appropriate. The operational environment restrictions assumed by this PP and the capabilities of the host implementations support the choice of an EAL 2 set of assurance requirements.

6.2.2 Strength of Function Rationale

The minimum strength of function level SOF-basic was chosen because the TOE environment assumes an environment in which the threat of malicious software attacks aimed at discovering exploitable vulnerabilities is considered low. The strength of metric established for the authentication mechanism described in FIA_UAU.1 was defined to ensure the mechanism is of adequate strength to protect against authentication data compromise. The strength of function level and metric chosen are consistent with the security objectives of the TOE because the security objectives are derived from the TOE environment, which describes a low risk environment.

6.2.3 Dependency Satisfaction

Functional Components include all dependent requirements.

6.2.4 Traceability

Table 11 shows how the requirements for the TOE map to the security objectives.

Table 11 Mapping of Requirements to Security Objectives

Security Objectives **TOE Security Functional Requirements**	**O.ACCESS**	**O.AUDIT**	**O.DATA_PRO**	**O.DOC**	**O.EAL**	**O.IDENTITY**	**O.MANAGE**	**O.PASSWORD**	**O.SELF_PROTECT**
FAU_GEN.1		●							
FAU_SAR.1		●							
FAU_STG.1		●							
FDP_ACC.1	●		●						
FDP_ACF.1	●								
FDP_UCT.1			●						
FDP_UIT.1			●						
FIA_UAU.1						●			
FIA_UID.1						●			
FMT_MSA.1							●		
FMT_MSA.3							●		
FMT_MTD.1(1)							●		
FMT_MTD.1(2)							●	●	
FMT_SMR.1							●		
FPT_ITC.1			●						
FPT_RVM.1									●
FPT_SEP.1									●
FPT_STM.1		●							
FTP_ITC.1			●						
AGD_ADM.1				●					
AGD_USR.1				●					
ADO_IGS.1				●					
EAL 2Assurance Requirements (See Table 9)					●				

6.2.5 Suitability

In this section each security requirement is shown to be suitable to satisfy the security objectives.

O.ACCESS

The TOE shall control access to the user's mailbox configuration status and data from the desktop based on the user's email identity and handheld identifier.

FDP_ACC.1 and FDP_ACF.1 identify and define the policy, rules, and operations the TOE shall implement to control access to a user's email messages. The policy defined only allows the desktop user to access the user profile for which they are assigned.

O.AUDIT

The TOE shall provide the capability to detect, create, store, and review records of security relevant events.

The FAU_GEN.1, FAU_SAR.1, FAU_STG.1, and FPT_STM.1 together provide an audit capability that generates and record security relevant events as defined in FAU_GEN.1. FAU_SAR.1 requires the ability for the audit records to be reviewed. FAU_STG.1 requires the audit records be protected. FPT_STM.1 is included to satisfy a dependency.

O.DATA_PRO

The TOE shall protect private key data transmitted from the TOE to other external components such as the Handheld and the mail server.

O.DATA_PRO is satisfied by requiring the protection of private keys from unauthorized disclosure (FDP_UCT.1, FPT_ITC.1) and modification (FDP_UIT.1) when transmitted and received.

FDP_ACC.1 and FTP_ITC.1 are included to satisfy dependencies.

O.DOC

Guidance documentation provided to authorized users and administrators will detail the proper installation and use of the TOE to minimize the security risks within its intended environment.

AGD_ADM.1 requires that the TOE vendor prepare guidance documentation for the authorized administrator. AGD_USR.1 requires that the TOE vendor prepare guidance documentation for the user. ADO_IGS.1 specifies installation and generation procedures.

O.EAL

The TOE must be structurally tested, shown to be resistant to obvious vulnerabilities, and be documented with sufficient design, test, and configuration documentation.

The assurance requirements for EAL 2 listed in Table 9 require that the TOE be designed and tested to conform to EAL 2. The EAL 2 requirements satisfy the security objective for a structurally tested, shown to be resistant to vulnerabilities, and a documented TOE.

O.IDENTITY

The TOE shall uniquely identify and authenticate each user of the system. The TOE shall not allow any user actions to be performed before the TOE verifies the identity of the user.

FIA_UAU.1 and FIA_UID.1 require a user to identify and authenticate themselves to the Desktop before any action can be taken.

O.MANAGE

The TOE will provide adequate management features for its security functions and the wireless two-way email system.

O.MANAGE is satisfied in two parts. FMT_MSA.1, FMT_MSA.3, and FMT_MTD.1(1) are necessary management functions required to support the email access control policy defined by FDP_ACC.1. These requirements allow the administrator to identify users and associate them to user profiles. FMT_MTD.1(2) is necessary to support the wireless two-way email system such that the Desktop provides the interface to define desktop policy for passwords.

FMT_SMR.1 is included to satisfy dependencies.

O.PASSWORD

The TOE will use an authentication mechanism that cannot be easily compromised in a low threat environment.

O.PASSWORD is satisfied by FMT_MTD.1(2) in which the Desktop must provide an interface to define a desktop policy for password strength, failed attempts, and password expiration.

O.SELF_PROTECT

The TOE must protect itself from unauthorized modification and access to its functions and data.

FPT_SEP.1 requires the TOE to protect itself by maintaining its own execution domain and protecting itself from external interference and tampering of TSF code and data structures from untrusted software (subjects). FPT_RVM.1 ensures that all actions required for policy enforcement are validated by the TSF and cannot be bypassed (compromised).

6.2.6 Explicit Requirements Rationale

The profile contains no extended requirements.

7 Acronyms

CC - Common Criteria
CM – Configuration Management
COTS – Commercial-Off-The-Shelf
DoD – Department of Defense
EAL - Evaluation Assurance Level
IT - Information Technology
NSA – National Security Agency
OS – Operating System
PP - Protection Profile
SF - Security Function
SFP - Security Function Policy
SFR – Security Functional Requirement
SOF - Strength of Function
SSO – Site Security Officer
ST - Security Target
TBD – To be determined
TOE - Target of Evaluation
TSC - TSF Scope of Control
TSF - TOE Security Functions
TSFI - TSF Interface
TSP - TOE Security Policy

8 References

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.
[2] Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.
[3] Wireless Two-Way Electronic Mail Handheld Protection Profile, Version 1.0, dated June 2002.
[4] Wireless Two-Way Electronic Mail Server Protection Profile, Version 1.0.dated June 2002.

9 Acronyms

CC - Common Criteria
CM – Configuration Management
COTS – Commercial-Off-The-Shelf
DoD – Department of Defense
EAL - Evaluation Assurance Level
IT - Information Technology
NSA – National Security Agency
OS – Operating System
PP - Protection Profile
SF - Security Function
SFP - Security Function Policy
SFR – Security Functional Requirement
SOF - Strength of Function
SSO – Site Security Officer
ST - Security Target
TBD – To be determined
TOE - Target of Evaluation
TSC - TSF Scope of Control
TSF - TOE Security Functions
TSFI - TSF Interface
TSP - TOE Security Policy

10 References

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.
[2] Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.